LA-UR-19-22469
Approved for public release; distribution is unlimited.

Title:	Comprehensive Security Briefing
Author(s):	Vigil, Robyn Ashlee
Intended for:	Presentation Web
Issued:	2019-03-18

Los Alamos
NATIONAL LABORATORY
EST. 1943

Comprehensive Security Briefing

SECURITY AWARENESS PROGRAM

UNCLASSIFIED

NNSA National Nuclear Security Administration

Briefing Objectives

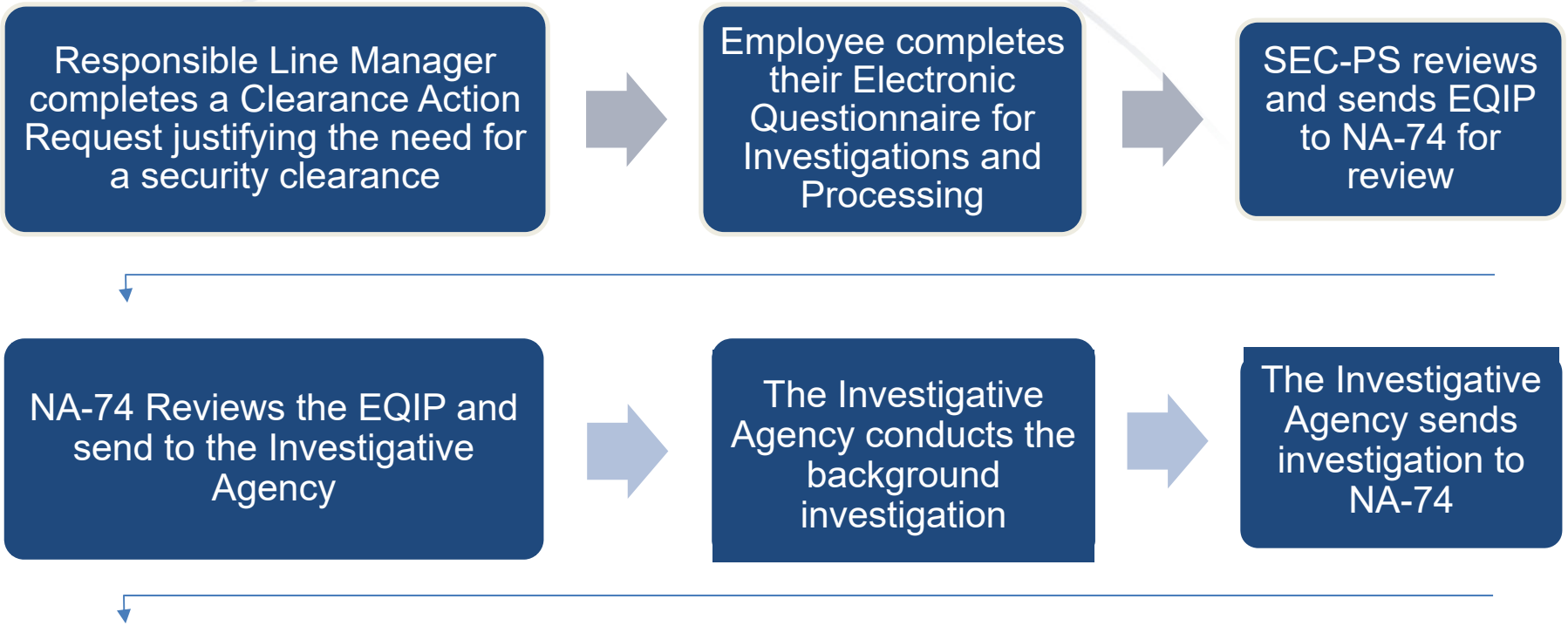
- Understand your security responsibilities
- Be aware that you can be held liable for the failure to protect classified matter
- Know where to get answers to your security questions

Why is this important?

Personnel Security

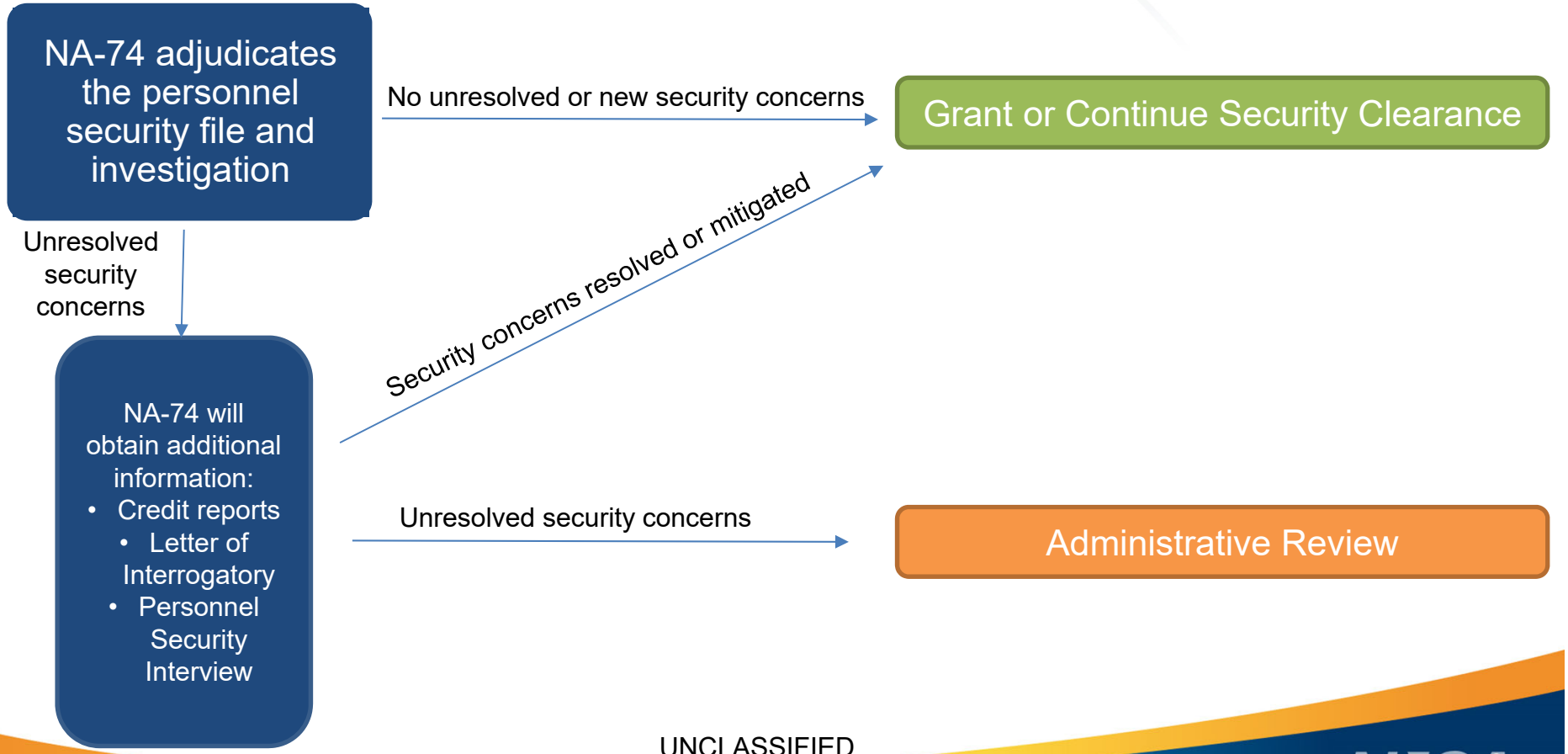
The Personnel Security group works to mitigate the risk individual workers pose by using a unique set of policies and procedures to confirm identity and citizenship, issue security badges, process clearances, and monitor human reliability for workers handling our nation's most sensitive nuclear materials.

Personnel Security
The Access Authorization Process



Continues on next slide.

Personnel Security
The Access Authorization Process cont.



Personnel Security
Access Authorization Process cont.

Adjudication:

The process directly following a background investigation where the investigation results are reviewed to determine if a candidate should be awarded a security clearance, or be suitable for a public trust position.

Personnel Security

Access Authorization Process cont.

Guidelines for Determining Eligibility for Access to Classified Information

A. Allegiance to the U.S
B. Foreign Influence
C. Foreign Preference
D. Sexual Behavior
E. Personal Conduct
F. Financial Considerations
G. Alcohol Consumption
H. Drug Involvement
I. Emotional, Mental, and Personality Disorders
J. Criminal Conduct
K. Security Violations
L. Outside Activities
M. Misuse of Information Technology Systems

Personnel Security
Access Authorization Process cont.

Administrative Review

Process by which the subject has an opportunity to present their case before an administrative review judge who makes the final determination regarding the eligibility to obtain or maintain a security clearance.

Due Process Rights

- Notified of the reason(s) for an unfavorable security clearance decision
- Given an opportunity to respond
- Notified of any appeal rights

Personnel Security
Access Authorization Process cont.

Reinvestigation

Individuals with access authorization are reevaluated to determine their continued need for access and eligibility every five years.

Personnel Security
Reporting Requirements

The following must be reported to Personnel Security within one business day of the reportable condition(s) by completing PERSEC F 5633.4 and providing a copy of all pertinent documentation.

Personnel Security
Reporting Requirements cont.

- Legal action effected for a name change
- Any change in citizenship status
- Any use of an illegal drug, or use of a legal drug in a manner that deviates from approved medical direction
- Any arrests, criminal charges (including dismissed charges), citations, tickets, summons or detentions by Federal, State, or other law enforcement authorities (including Tribal authorities) for violations of law within or outside of the US
  - Traffic violations for which a fine of up to $300 was imposed need not be reported, unless the violation was alcohol- or drug-related

Personnel Security
Reporting Requirements cont.

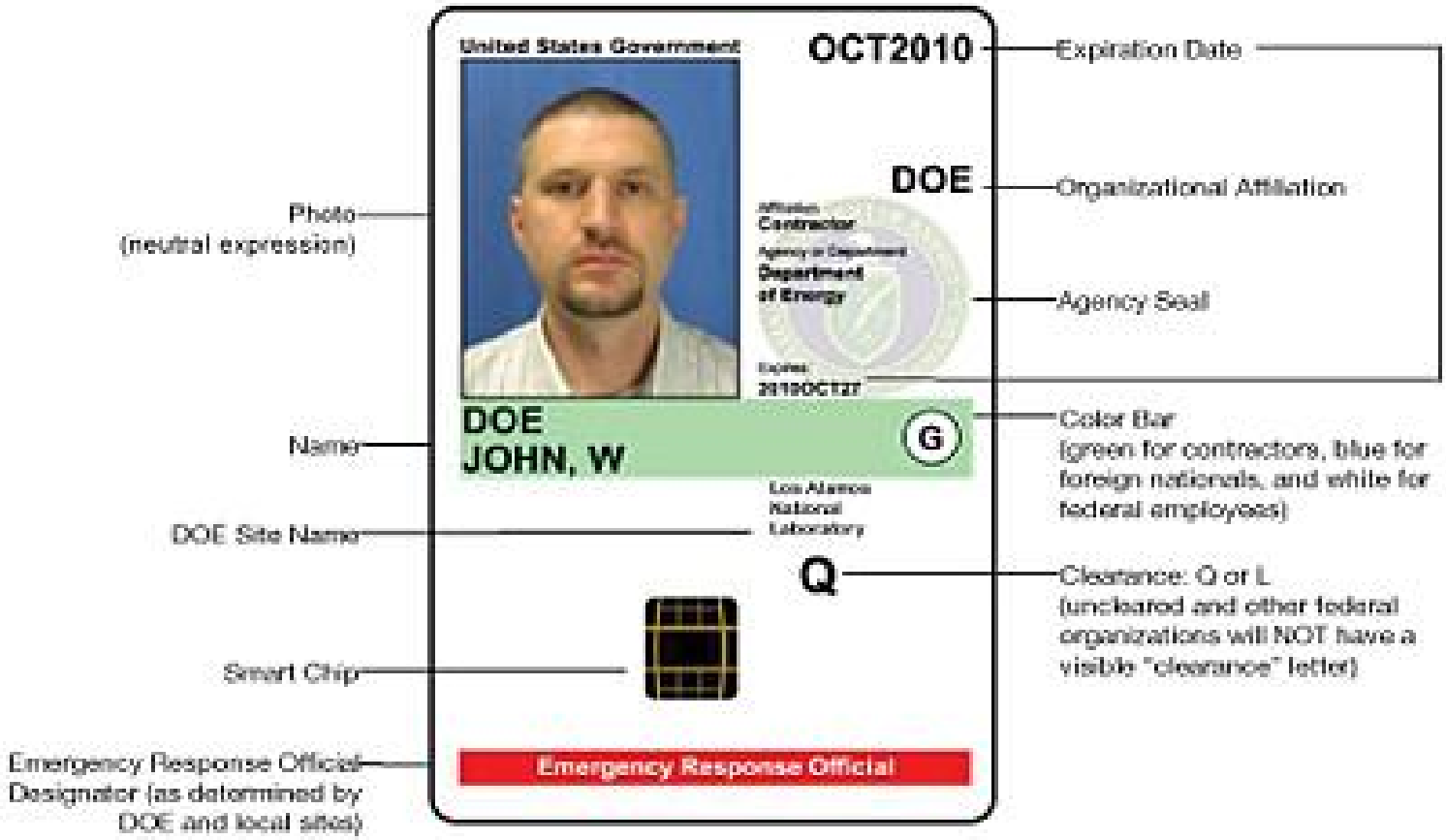
- An immediate family member assuming residence in a sensitive country
- Hospitalization for mental health reasons or treatment for drug or alcohol abuse
- Employment by, representation of, or other business-related association with a foreign or foreign-owned interest or non-US citizen or other individual who is both a US citizen and a citizen of a foreign country
- Personal or business-related filing for bankruptcy
- Garnishment of wages
- Any situations or incidents that may have the tendency to impact a worker's eligibility for a security clearance

Personnel Security
Reporting Requirements cont.

- Spouse-like cohabitations and marriages

Within 45 business days by completing DOE F 5631.34, Data Report on Spouse/Cohabitant and sending it to Personnel Security.

Personnel Security
Badge Holder Responsibilities
HSPD-12



Personnel Security
Badge Holder Responsibilities

- Wear your badge, photo-side out, above the waist, on the front side of the body when on Laboratory property
- Remove you badge and protect it from public view when leaving the Laboratory
- Use the badge as a means of identification for official government purposes only
- Never photograph or photocopy your badge
- Present your badge at the request of the Protective Force, line management, Laboratory host, or Personnel Security Specialist

Personnel Security
Badge Holder Responsibilities

- Always bring your badge with you to the Laboratory. Limit the number of instances a temporary badge is issued
- Return any badge to the Badge Office
- Report a lost badge to the Badge Office within 24 hours or the next business day
- If you suspect that your badge was stolen, report it to your Deployed Security Officer or the Security Incident Team as well as the Badge Office within 24 hours or the next business day
- Upon Termination, sign your Security Termination Statement and return your badge to Personnel Security

Personnel Security
Substance Abuse Program

As a DOE laboratory with a national security mission, LANL cannot tolerate illegal activity and must ensure a work environment that is free from unauthorized or illegal use, possession, or distribution of alcohol or controlled substances.

Any use of an illegal drug, or use of a legal drug in a manner that deviates from approved medical direction is prohibited.

DOE/NNSA may terminate or refuse to grant or renew a security clearance for a worker who is an unlawful user of a controlled substance, or an addict.

Personnel Security
Substance Abuse Program cont.

In support of the Laboratory's commitment to maintain a drug and alcohol-free workplace, the Laboratory requires:

- Pre-employment drug testing
- Random drug and alcohol testing
- Drug and/or alcohol testing based on reasonable suspicion
- Post-accident drug and/or alcohol testing

If a LANL badge holder fails to appear to a scheduled drug and/or alcohol test, the test will be treated as a confirmed positive.

Personnel Security
Substance Abuse Program cont.

New Mexico has passed legislation allowing for the use of marijuana for medical purposes in certain circumstances; however, marijuana use and possession for any reason remains illegal under Federal law. Therefore, the use, possession, and distribution of marijuana is **prohibited**, including any of its derivatives (e.g. CBD).

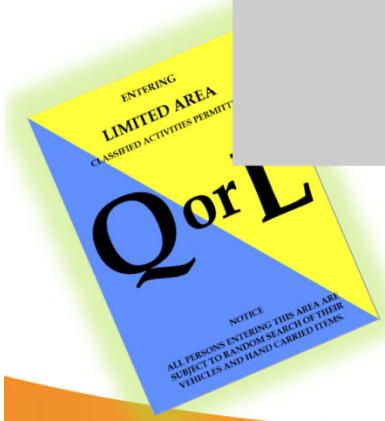
If you suspect you may have been exposed to an illegal drug, notify your responsible line manager and Personnel Security on your first day back to work.

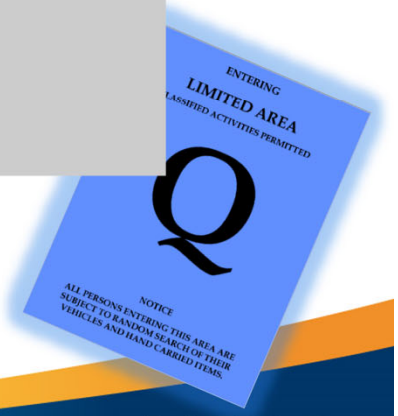
Security Training

- Laboratory workers who hold a security clearance are required to complete the Annual Security Refresher
  - Access Authority is tied to this training
- E-mail reminders 60 & 10 days prior to expiration and the day of expiration
- 90 days passed expiration = clearance termination

Security Areas

LANL's Graded Approach to Security Areas





Controlled Portable Electronic Devices (PEDs)

A device that is easily portable, and can store, read, write, record, and/or transmit information. Examples include, but are not limited to:

- Cell phones
- Smart watches
- Cameras
- Laptops
- Pagers
- Two-way radios
- Medical device
- Tablets

Responsibilities

- Verify that a Controlled PED is allowed in an area before introducing it into the area.
- Follow PEDs Rules of Use
- Ensure visitors are aware of Controlled PED requirements

Controlled PEDs cont.

In general, **The enablement of Bluetooth and WiFi is only allowed in GAAs and Privately-owned PEDs are NOT permitted in Security Areas.**

Table 1. Use of Controlled PEDs on Laboratory Property
The RLM may determine need for additional restrictions and post those restrictions.

Level	Description	Access to Physical Area	Allowed LANL Networks
1	**Privately-owned**. LANL does not control the device. [Use of medically-necessary Controlled PEDs requires an approved exception before entering a Limited Area or above]	General Access Area (GAA) or Property Protection Area (PPA)	Visitor Network only RLM issues credentials
2	**US Federal Government-owned and property-tagged.** Administrative controls apply, LANL has the right to confiscate and shred if contaminated	General Access Area (GAA) or Property Protection Area (PPA)	Visitor Network only RLM issues credentials
3	**LANL-owned and property-tagged, and configured to LANL standards**. May have a working microphone, camera and/or wireless.*	PA and LA permitted unless the RLM restricts access.	LANL Unclassified Yellow Network, with appropriate authorization (laptops)
4	**LANL-owned, property-tagged, and configured with ISSM-approved** disablement of the camera, microphone and wireless** (see sticker on Controlled PED).*	PA, LA and Vaults/VTRs permitted unless the RLM restricts access.	LANL Unclassified Yellow Network, with appropriate authorization (laptops)

Prohibited Articles

The following prohibited articles must not be brought on Laboratory property:

- Firearms
- Dangerous weapons and explosives
  - (including knives with blades longer than 2.5 inches)
- Alcoholic beverages
- Controlled substances
- Items prohibited by law

Protective Force

The Protective Force (PF) provide security services to the Laboratory by providing physical security for facilities, fixed and roving patrols, access control and vehicle inspections, and security emergency response.

Cooperation Requirements

All personnel on Laboratory property are required to cooperate with PF officers on security matters and participate fully in the Laboratory's security programs. All LANL employees must follow the directions of the PF officers. Arguing, using inappropriate hand gestures, and inappropriate language is not tolerated.

Escorting

By holding a security clearance, you may be required to escort an uncleared US citizen into Security Areas. To be an eligible escort you must:

- Hold the appropriate access authorization
- Be aware of site-specific procedures
- Be trained in the Laboratory escort procedures (UTrain Course #18366)
- Ensure that site-specific requirements for escorting in the area are followed

Escorting cont.

Prior to the visit, escort must:

- Meet the escorted visitor outside of the Security Area
- Ensure that the escorted visitor possess a valid badge
- Brief the escorted visitor on any relevant prohibited and controlled articles
- Brief the escorted visitor on security and safety requirements for the facility

Escorting cont.

During the visit, the escort must:

- Ensure that the escorted visitor displays a valid badge at all times
- Maintain visual and aural control of the escorted work at all times
- Prevent unauthorized access to sensitive or classified matter by the escorted visitor
- Prevent the compromise of unauthorized disclosure of sensitive or classified matter
- Mitigate and report any violations of escorting requirements
- Ensure that the number of escorted workers per escort meets the established requirement for the area and activity

Escorting cont.

Ending a visit, the escort must:

- Retrieve any badge issued to the escorted visitor. If the badge was issued by the Badge Office within one business day
- Comply with any site-specific requirements for exiting the area with an escorted visitor

Special Nuclear Material Protection

The Nuclear Material Control & Accountability (NMCA) Program provides graded levels of control for accountable nuclear material (NM) and special nuclear material (SNM) based on the material type, quantity, and form. The program seeks to deter and detect theft or diversion of accountable material.

Classification

Now that you hold a security clearance, you are eligible for access to classified information and must be familiar with DOE and Laboratory policies to ensure classified information and controlled unclassified information (CUI) is correctly identified so that it can be protected.

Basis for Classification Program

DOE Orders

- DOE O 475.2B: Identifying Classified Information
- DOE O 471.1B: Identification and Protection of Unclassified Controlled Nuclear Information
- DOE O 471.3: Identifying and Protecting Official Use Only Information

LANL Policies

- P204-1 Controlled Unclassified Information
- P204-3 Classification of Matter

Other References

- P204-5 Protection of Weapon Use Control Information (Sigma 14 & 15)
- 10 CFR 1045, Nuclear Classification and Declassification
- 32 CFR 2001, Classified National Security Information

Classification Subject Areas

The Laboratory uses and produces information in many classified subject areas including:

- Nuclear weapon, design, production, use control, testing, and stockpile management.
- Nuclear terrorism and counterterrorism
- Nuclear proliferation detection research and development
- Counter chemical, biological, and radiological weapons-of-mass-destruction research and development
- Radiological emergency response
- Nuclear safeguards and Security
- Intelligence and counter-intelligence

Your Line Manager is responsible for ensuring that you become familiar with the specific classified information you are likely to encounter.

Classification cont.

Classification is the means by which the United States Government identifies certain information that needs to be protected in the interest of national security by authority of the Atomic Energy Act, the National Security Act, and Executive Orders on National Security Information.

Classified Matter – the physical form of classified information.

Classification Categories

There are four distinct categories of classified information, based on the authorization basis and the nature of the information.

1. Restricted Data (RD)
2. Formerly Restricted Data (FRD)
3. Transclassified Foreign Nuclear Information (TFNI)
4. National Security Information (NSI)

Classification Categories cont.

The Atomic Energy Act defines two categories of classified information related to nuclear weapons: Restricted Data and Formerly Restricted Data.

Restricted Data (RD)

Specific information regarding the development and production of nuclear weapons, including but not limited to:

- Shapes, dimensions, materials, masses, etc. of components inside bomb case, or reentry body/reentry vehicle
- Computer codes used to design nuclear weapons or calculate nuclear weapon performance

Classification Categories cont.

Formerly Restricted Data (FRD)

Specific information regarding the military utilization of nuclear weapons, including but not limited to:

- Actual quantities of active and retired nuclear weapons
- Storage locations and deployment
- Nuclear targeting information

Classification Categories cont.

Executive Order 13526 describes two classification categories: Transclassified Foreign Nuclear Information and National Security Information.

Transclassified Foreign Nuclear Information (TFNI)

Certain information collected by the US intelligence community regarding foreign nuclear capabilities.

Classification Categories cont.

National Security Information (NSI)

Specific information within the following categories that has been identified by U.S. Government Agencies as so sensitive that the release would cause harm to national security :

- Military plans, operations
- Scientific, technological, or economic matters relating to national security
- Safeguarding nuclear materials or facilities
- Vulnerabilities affecting “critical infrastructure”
- Development, production, or use of weapons of mass destruction (“WMD”, including chemical, biological, radiological, and nuclear)
- Intelligence activities, sources or methods, or cryptology
- Foreign government information, foreign relations or foreign activities of the United States

Classification Levels

The U.S. Classification system has three classification levels which indicate the relative importance of classified information to national security and the specific security requirements applicable to them. Classification levels apply to all four classification categories.

Classification Levels

- **Top Secret (TS) –** The unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security.
- **Secret (S) –** The unauthorized disclosure of which reasonably could be expected to cause serious damage to national security.
- **Confidential (C) –** The unauthorized disclosure of which reasonably could be expected to cause damage to national security or could be reasonable expected to cause undue risk to the common defense and security for RD and FRD.

Classification
Classified Matter Categories & Levels

	Restricted Data (RD)	Formerly Restricted Data (FRD)	National Security Information (NSI)
Top Secret (TS)	Q	Q	Q
Secret (S)	Q	Q/L	Q/L
Confidential (C)	Q\L	Q\L	Q\L

Classification
Access Requirements

The three main requirements for access to classified matter include:

- Appropriate access authorization
  (i.e. Q security clearance; L security clearance)
- Need to know to perform official duties
- Relevant access approvals
  (e.g. sigma authorities; SCI clearance)

Derivative Classification

The Laboratory's Classification Officer delegates authority to apply classification instructions through the practice of Derivative Classification to individual Laboratory employees. Derivative Classifiers (DCs) at LANL are authorized to classify LANL work products in certain, limited subject areas.

Classification Authorities

Derivative Classifier (DC)

- DC authority is required to determine if a LANL document contains classified information or if a document should be upgraded to a higher level or category.

Derivative Declassifier (DD)

- Derivative Declassification authority is required to determine if a LANL document should be declassified or downgraded to a lower level or category.

Classification Authorities

- The **Classification Officer** and **Classification Analysts** may derivatively classify and derivatively declassify and downgrade LANL documents in any and all classified subject areas.
- The **Classification Officer** and **Classification Analysts** are the only Laboratory employees who are authorized to approve the public release of unclassified LANL documents generated in a classified subject area.
- The **Classification Officer** ensures that every Lab employee with access to classified email services is trained to derivatively classify emails (**E-mail DCs**).

Classification Review Requirements
Your Responsibilities

All potentially classified documents that you generate in a classified subject area must be reviewed by a DC. You must also have a document reviewed when:

- You have an unmarked document you believe may contain classified information
- You believe a document should be classified at a higher level and/or category
- You extract information from a classified document
- You print a document from a classified system
- You incorporate information from open literature that is in a classified subject area into a new document

Classification Review Requirements Your Responsibilities cont.

- If a DC does not immediately review your document, you must mark it as a *working paper* and protect it at the highest potential level and category.
  - A DC must review the working paper before it is retained for more than 180 days from the date of the last change, released outside the originating activity, or filed permanently.

Declassification

Declassification of information is the determination by appropriate authority that information no longer requires classification. Declassification requires two independent reviews. Only a Derivative Declassifier (DD) has the authority to change markings on the subject matter to reflect the new level and/or category. A few required declassification reviews include (please see DOE O 475.2B, Attachment 4 for an all-inclusive list):

- A classified document that is being prepared for declassification
- A classified document that is being prepared as a redacted version
- An NSI document or material marked for declassification with a specific date or event that has passed prior to the actual declassification date (single review only)

Once declassified, material can be shared with uncleared colleagues.

Challenging Classification Decisions

During your work, you may come across classified information that you think should not be classified or is classified at an incorrect level or category.

When that happens, you are encouraged and expected to challenge the classification. You may start by discussing the classification decision with the Derivative Classifier who made the decision to better understand the classification.

If you prefer, you may discuss the classification decision with the Classification Officer or submit a written challenge to the Classification Officer. You also have the option to submit a written challenge directly to the Director of the Office of Classification at any time. Under no circumstance will you be subject to retribution for a challenge.

Controlled Unclassified Information

Controlled Unclassified Information (CUI) is information that is unclassified, yet subject to safeguarding:

- Unclassified Controlled Nuclear Information (UCNI)
- Official Use Only (OUO)
  - Personal Identifiable Information (PII)
  - Export Controlled Information (ECI)

Unclassified Controlled Nuclear Information

UCNI is certain information concerning nuclear facilities, materials, weapons, and components.

UCNI Authorities

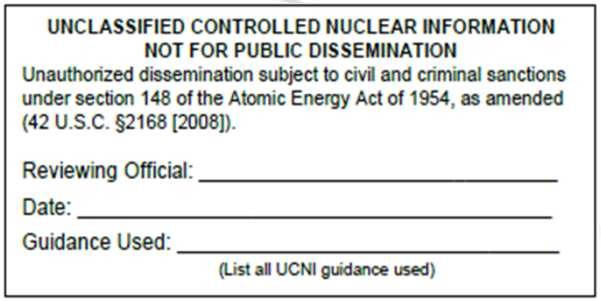
Much like DCs are required to determine if a LANL document contains classified information, a LANL UCNI Reviewing Official authority is required to determine if a document contains UCNI.

UCNI

Access Requirements

Need to Know

Marking Requirements


UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION
NOT FOR PUBLIC DISSEMINATION
Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. §2168 [2008]).
Reviewing Official: _____
Date: _____
Guidance Used: _____
(List all UCNI guidance used)

- Documents containing UCNI have UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION marked on the front, back, and internal pages.
- There is also a front marking that identifies the authority used to make the UCNI determination.
- Email containing UCNI will have UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION at the beginning of the body of the email.

UCNI
Additional Safeguards

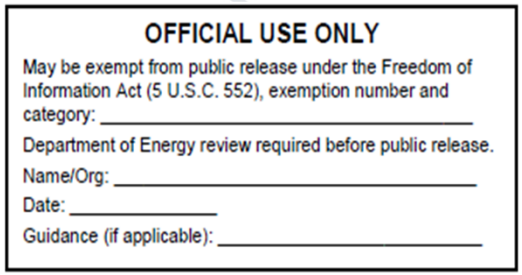
- Ensure no unauthorized access
- When outside of secured area, must be stored in a locked receptacle
- Must only be reproduced to the minimum extent necessary
- Must be encrypted if transmitted electronically (e.g. email, telephone, fax) outside of the LANL Yellow or Red Network
- Must only be destroyed by shredding, burning, or any approved method for classified

Full requirements for identifying and protecting UCNI can be found in 10 CFR Part 1017 and DOE O 471.1B.

Official Use Only

OUO Access Requirements

- Need to Know
- ECI – U.S. Citizens


OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: _____

Department of Energy review required before public release.

Name/Org: _____

Date: _____

Guidance (if applicable): _____

Marking Requirements

- Documents containing OUO information have a front marking that identifies the FOIA Exemption Number and Category, the name of the person making the determination, and (if the determination is made by a DC), the name of the classification guide used to make the determination.
- Email containing OUO information will have OUO at the beginning of the body of the email.

OUO
Additional Safeguards

- Ensure no unauthorized access
- Must be destroyed by shredding or burning

Other Government Agency CUI

At LANL, you may encounter other Government Agency CUI. Please see the Classification Office for further details.

Classified Matter Protection and Control/Operational Security

The Classified Matter Protection and Control (CMPC) program and the Operations Security (OPSEC) program exist to ensure the proper use and protection of classified and sensitive information.

- The CMPC program directs how classified matter is accessed, stored, generated, marked, reproduced, received and transmitted, destroyed and accounted for.
- The OPSEC program assists workers in identifying and protecting unclassified information that could be useful to the Laboratory's adversaries.

CMPC
Responsibilities

Employees with access to classified information are responsible for:

- Completing the Classified Matter Protection Training (UTrain Course # 16028) prior to receiving access to classified matter and the Classified Matter Protection and Control User Refresher Training (UTrain Course #35043) every two years thereafter
- Protecting classified matter from unauthorized physical, visual, or aural access
- Conducting classified discussions and work only in Security Areas

CMPC
Storage of Classified Matter

When not in approved storage, all classified information must be under the direct control of a worker who meets the access authorization requirements.

While procedures for closing and securing a storage container will vary depending upon the type of container and type of lock in use:

- close all drawers and ensure they are fully closed and latched
- Turn the container's combination dial to the left (counter-clockwise) one complete revolution and then to the right (clockwise) one complete revolution.

CMPC
Storage of Classified Matter cont.

- Attempt to open the door/drawer with the combination dial by turning and pulling on the handle. Attempt to open the other drawer(s) by pulling on the drawer handle(s) while pressing in the button.
- After checking to make sure it is locked, record the completion of the storage container closure by completing the “Closed By” section of Standard Form (SF) 702 (1692a).

CMPC
End-of-Day Checks

- When an end-of-day check is performed on a storage container, the worker assigned to performing the check must ensure that each storage container used to store classified matter is properly secured at the end each workday, whether or not the storage container was accessed for the work day.
- Checks may be performed by a worker other than the user who opened and/or closed the storage container. If an employee opens a storage container after normal operating hours, on a weekend or any other non-work day (i.e., when LANL is closed for a holiday or snow day), an end-of-day check must be performed.
- End-of-day checks are not required for Government Services Administration (GSA)-approved storage containers kept within vaults or vault-type rooms (V/VTRs). If the vault or VTR was not opened for the day, however, only the V/VTR itself must be checked.

CMPC
Responsibilities cont.

- Follow the proper procedures for originating, marking, transmitting, accounting for, reproducing, and destroying classified matter as delineated in P204-2.

Table 2. Classified Document Standard Markings

Required Marking	Front Cover Page (optional)	Title Page (optional)	First Text Page	Interior Text Pages	Back of Text Page	Back Cover Page (optional)	Routing Sheet (optional)
Classification Level: Top Secret (TS), Secret (S), or Confidential (C)	Top and bottom of page	Top and bottom of page	Top and bottom of page	Top and bottom of each page	Top and bottom of outside back page	Top and bottom of outside back page	Top and bottom of outside back page
Classification Category and Admonishment: Restricted Data (RD) or Formerly Restricted Data (FRD) *Note:* National Security Information (NSI) does not require category marking on documents	For RD and FRD, lower left side of page	For RD and FRD, lower left side of page	For RD and FRD, lower left side of page	Top and bottom of page along with Classification Level and Category (i.e., Secret/RD)	Not required (recommended)	Not required (recommended)	Not required (recommended)
Unique identification number: for accountable documents and Classified Removable Electronic Media (CREM)	Preferably upper right corner	Preferably upper right corner	Preferably upper right corner	Not required	Not required	Not required	Not required
	Unique identifier is required only on the first page of text and on the front of CREM.						
Date of Preparation	Any location	Any location	Any location	Not required	Not required	Not required	Not required
	Date of preparation is required only on the first page of documents.						
Originator Identification: Use LANL letterhead or include complete mailing address and organization.	Any location	Any location	Any location	Not required	Not required	Not required	Not required
	Originator identification is required only on the first page of text.						
Title or Subject *Note:* When possible, titles should be unclassified.	Any location	Any location	Any location	Not required	Not required	Not required	Not required
	Title or subject is required only on the first page of text.						
Derivative Declassifier	Above Classifier Information	Not required	Not required	Any location	Any location	Not required	Not required

UNCLASSIFIED

Classification & CMPC Assistance

Derivative Classifiers (DCs)

A list of DCs can be found on the Classification Website.

Information Protection Group (SAFE-IP) & Classification Officer

SAFE-IP maintains the Laboratory's Institutional capabilities and resources for identifying classified and controlled unclassified information. 505-667-5011

Classified Matter Custodians (CMCs)

Organizations throughout the Laboratory have CMCs, responsible for assisting in the protection and control of classified matter. CMCs are resources to assist Laboratory workers in the generation, marking of, reproduction, control, protection, storage, and destruction of classified matter.

Classification
Unauthorized Disclosure

An unauthorized disclosure is whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States, any classified information.

Title 18, USC, Section 798

UNCLASSIFIED

Classification

Unauthorized Disclosure cont.

May result in violations of U.S. Criminal Laws, such as sections 641, 793, 794, 798, 952, and 1924, title 18, United States Code. and section 783(b), title 50, U.S.C.

Punishments for a person convicted of this violation, include, but are not limited to:

- Fine of not more than $10,000, per count
- Imprisonment of not more than 10 years, per count
- Forfeiting any property constituting, or derived from, any proceeds the person obtained as the result of such violation
- Forfeiting any property the person used or intended to use in such violation

Classification
Potential Unauthorized Disclosure

A PUD is the exposure of classified or controlled unclassified information to people who are not authorized users of the information or who have no need to know.

Examples of PUDs:

- Disseminating information without having it reviewed
- Creating “classified by association”
- Forwarding emails or attachments to those who do not have a need to know

Classification PUD cont.

How to best prevent a PUD:

- Always obtain derivative classification reviews for potentially classified and controlled unclassified information.
- Be aware of the combination of information and how information that alone can be unclassified, yet when combined can potentially become classified.
- Utilize the safeguards in place for preventing PUDs, such as Entrust, LANL's encryption software.
- Be cognizant of the information you discuss/transmit and your entire audience.

Classification
DOE General Policy 16: No Comment

Commenting on classified information that is in open literature, or attempting to prevent its further dissemination, could result in great damage to national security than would occur if no comment were made about the information.

Therefore, all authorized holders of classified information shall not confirm nor expand upon the classification status or technical accuracy of classified information.

- The appearance of such information in the public domain or open sources does not automatically declassify it
- The selective use of “no comment” may result in confirming classified information

Classification
GOE General Policy 19

You must also be aware of DOE's policy (GEN-19) that essentially prohibits any individual with current or past authorized access to RD or FRD information from releasing into the public domain information regarding theory, operation, or design of nuclear weapons.

Information Security

All Laboratory General Users are required to actively comply with all information security policies and procedures set forth by DOE and the Laboratory. When you use a Laboratory system, you agree to the terms and conditions of use. Good reminders for information security include:

- Utilizing Government computing systems for official work, except in emergencies threatening loss of life or government personal property, or for incident use (as specified in P821)
- Protecting systems from unauthorized access (e.g. locking your computing system when not in use; following the Laboratory's password policy)
- Installing only information-architecture-approved hardware and software

Information Security cont.

- Be aware of the threats to information security (e.g. phishing)
- Do not download attachments or click on links in suspicious emails
- Do not insert non-government USB devices into government computing systems
- Promptly report any suspected information security incidents to the Security Incident Team (SIT)

Incidents of Security Concern

Incidents of Security Concern are actions, inactions, or events that:

- Pose threats to national security interests and/or critical DOE assets;
- Create potentially serious or dangerous security situations;
- Degrade the effectiveness of the safeguards and security (S&S) program; or
- Adversely impact that ability of organizations to protect DOE S&S interests

Incidents of Security Concern cont.

<u>Laboratory workers and visitors are required to report any known or potential incidents of security concern</u> to the Security Incident Team (SIT) or a Deployed Security Officer (DSO)/Security Program Lead (SPL) and their RLM. Reports are not allowed to be made via email or voicemail.

Security Incident Team
505-665-3505

If an incident of security concern is discovered outside of normal business hours, it must be reported to the **On-Call Duty Officer (OCDO) at 699-4094.**

Laboratory workers and visitors must ensure that information regarding known or potential security vulnerabilities is properly protected.

Incidents of Security Concern cont.

Administrative Actions

Security Infraction

An in advertent act or omission involving failure to comply to comply with DOE or Laboratory safeguards and security procedures.

- Permanent part of DOE personnel file
- Disciplinary action
  - Counseling
  - Termination

Office of Counterintelligence

The Office of Counterintelligence (OCI) protects the Laboratory from efforts by foreign intelligence services and terrorist entities to acquire sensitive and/or classified information.

Office of Counterintelligence
Reporting Requirements

All LANL personnel, subcontractors, and foreign visitors are required to report the following:

- Professional and substantive personal relationships with sensitive country foreign nationals.
- Substantive financial relationships, either one-time or ongoing with citizens of sensitive countries.
- Official and unofficial travel to sensitive countries.
- Any attempt by an unauthorized person to gain access to classified information.
- Anomalies - Foreign power activity or knowledge inconsistent with the expected norm that suggests foreign knowledge of U.S. national security information, processes, or capabilities.

Office of Counterintelligence

Elicitation

Elicitation is the process of calling forth or drawing out information. In the espionage trade, elicitation is the technique of gathering intelligence through what appears to be normal contact. It is important to be aware of common elicitation techniques:

- Appealing to one's ego
- Expression of mutual interest
- Deliberate false statements
- Volunteering information
- Assumed knowledge

Office of Counterintelligence

Recruitment

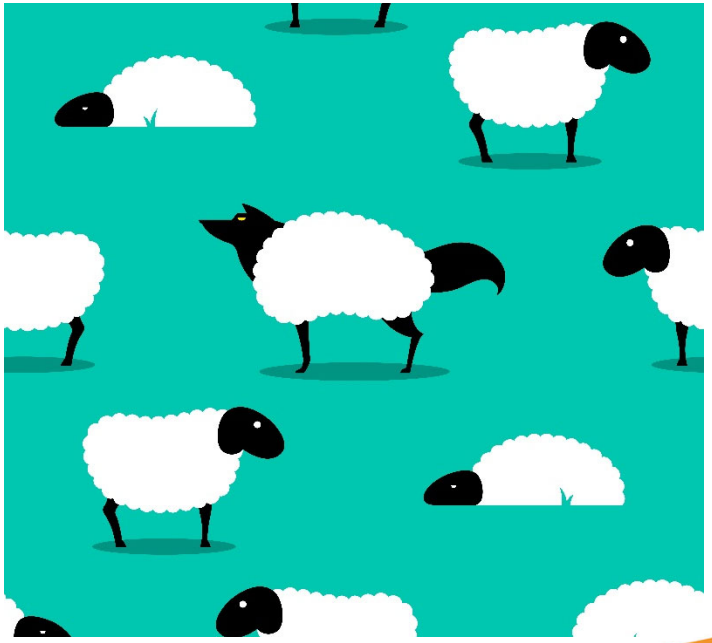
Foreign Intelligence Services (FIS) are constantly evaluating potential human sources. If someone appears to have potential for development as a spy, serveral techniques or approaches may be used to recruit members:

- Financial considerations/greed
- Blackmail/hostage situations
- Appeal to national pride
- Exploitation of emotional involvement
- “False flag” approaches
- Approaches based on ideology
- Exploitation of American ideals
- Revenge/disaffection with job

Office of Counterintelligence
Insider Threat

"A threat posed to U.S. national security by someone who misuses or betrays, wittingly or unwittingly, their authorized access to any U.S. Government resource" Examples include damage through:

- Espionage
- Terrorism
- Unauthorized disclosure
- Loss or degradation of departmental resources or capabilities



Office of Counterintelligence
Insider Threat cont.

The FBI has identified several behavioral indicators of an insider threat, including, but not limited to:

- Without need or authorization, takes material home
- Inappropriately seeks or obtains material on subjects not related to their job duties
- Interest in matters outside the scope of their duties
- Unnecessarily copies material (especially if it is proprietary or classified)
- Works off hours without authorization
- Unreported foreign contacts
- Overwhelmed by life crises or career disappointments

Office of Counterintelligence

DOE employment gives you access to information or people that foreign governments value.

You are the first line of defense against foreign intelligence collection operations. Report suspicious behavior and activity by calling the Office of Counterintelligence at 505-665-6090.

If you see something, say something.

Safeguard and Security Resources

Defense Security Program Website:
http://int.lanl.gov/org/ddops/aldeshqss/defense-security/index.shtml

- **SD 200** Integrated Safeguards and Security Management
- **P 201-1** Minor Visitors on LANL Property
- **P 201-3** Reporting Known and Potential Incidents of Security Concern
- **P 201-4** Public Demonstrations
- **P 202-1** Security Areas, Property Protection Areas, and General Access Areas
- **P 202-2** Vaults and Closed Areas
- **P 202-4** Security Locks and Keys
- **P 202-5** Prohibited Articles
- **P 202-6** Security Escorting
- **P 202-7** Security Conditions
- **P 203-1** Security Badges
- **P 203-2** Security Clearances
- **P 203-3** Human Reliability Program
- **P 203-4** Counterintelligence Reporting Requirements
- **P 203-5** Incoming Classified Visits
- **P 203-6** Unclassified Foreign Visits and Assignments
- **P 203-7** Outgoing Classified Visits
- **P 203-9** Foreign Ownership, Control, or Influence (FOCI)
- **P 204-1** Controlled Unclassified Information
- **P 204-2** Classified Matter Protection and Control Handbook
- **P 204-3** Classification of Matter
- **PD 205** Nuclear Material Control and Accountability
- **P 805** Export Control

Standard Form 312
Classified Information Nondisclosure Agreement

All persons with authorized access to classified must sign this nondisclosure agreement as a condition to access.

- You may be entrusted with classified.
- You acknowledge your responsibility to protect classified from unauthorized disclosure.
- You understand that there are consequences for failure to protect classified.